

WHAT IS CLAIMED IS:

1 1. In a public key authentication system, a method of sending an
2 authenticated message to a recipient via a network, the method comprising:
3 digitally signing a message using a first private key associated with the sender;
4 retrieving a first certificate reference associated with a first certificate, the first
5 certificate including a first public key corresponding to the first private key, wherein the first
6 certificate and the associated first certificate reference are stored in a public key
7 infrastructure; and
8 transmitting to the recipient via the network an authenticated message
9 comprising the digitally signed message and the first certificate reference.

1 2. The method of claim 1, further comprising:
2 transmitting the first certificate via the network to the public key infrastructure
prior to transmitting the authenticated message.

1 3. The method of claim 1, wherein the first certificate reference is
2 determined from an identity of the sender and a serial number of the first certificate.

1 4. The method of claim 1 further comprising:
2 retrieving a second certificate reference to a second certificate, wherein the
3 second certificate is issued to an issuer of the first certificate, wherein the second certificate
4 and the associated second certificate reference are stored in the public key infrastructure; and
5 transmitting the second certificate reference as a further portion of the
6 authenticated message.

1 5. The method of claim 1, wherein the network is the Internet.

1 6. The method of claim 1, further comprising encrypting the message
2 using a second public key, wherein the recipient holds a second private key corresponding to
3 the second public key.

1 7. In a public key authentication system, a method for authenticating a
2 message received from a sender via a network, the received message including a digitally
3 signed message and a first certificate reference, the method comprising:

4 transmitting the first certificate reference to a public key infrastructure via the
5 network;
6 receiving from the public key infrastructure via the network a first certificate
7 corresponding to the first certificate reference, the first certificate including a first public key;
8 determining whether the first certificate is trusted; and
9 if the first certificate is trusted, authenticating the digitally signed message
10 using the first public key.

1 8. The method of claim 7, further comprising:
2 storing in a local keystore the first certificate reference and the first public key.

1 9. The method of claim 7, wherein the step of determining whether the
2 first certificate is trusted comprises:

3 identifying a first issuer of the first certificate;
4 comparing the first issuer to each of at least one trusted issuer; and
5 if the first issuer is the same as one of the at least one trusted issuer,
6 determining that the first certificate is trusted.

1 10. The method of claim 7, wherein the received message further includes
2 a second certificate reference, the method further comprising:

3 transmitting the second certificate reference to the public key infrastructure via
4 the network; and

5 receiving from the public key infrastructure a second certificate corresponding
6 to the second certificate reference, the second certificate including a second public key
7 associated with an issuer of the first certificate.

1 11. The method of claim 10, wherein the step of determining whether the
2 first certificate is trusted comprises:

3 determining whether the second certificate is trusted;
4 if the second certificate is trusted, using the second public key to authenticate
5 an issuer signature included in the first certificate, thereby verifying the first certificate; and
6 if the first certificate is verified, determining that the first certificate is trusted.

1 12. The method of claim 7, wherein the network is the Internet.

1 13. In a public key authentication system, a method for obtaining a public
2 key for authenticating a received message comprising a digitally signed message and a first
3 certificate reference, the method comprising:
4 determining whether the first certificate reference is stored within a local
5 keystore;
6 if the first certificate reference is stored within the local keystore:
7 retrieving from the local keystore a first public key associated with the
8 first certificate reference; and
9 if the first certificate reference is not stored within the local keystore:
10 transmitting the first certificate reference to a public key infrastructure;
11 receiving from the public key infrastructure a first certificate
12 corresponding to the first certificate reference, the first certificate including the first public
13 key;
14 determining whether to trust the first certificate; and
15 adding information to the local keystore, the information including at
16 least the first certificate reference and the first public key.

1 14. The method of claim 13, further comprising:
2 authenticating the digitally signed message using the first public key.

1 15. A method of operating a public key infrastructure, the method
2 comprising:
3 receiving a certificate from a first user;
4 computing a unique certificate reference from data contained in the certificate;
5 storing the certificate in association with the unique certificate reference;
6 receiving a request from a second user, the request including the unique
7 certificate reference; and
8 transmitting the certificate to the second user in response to the request.

1 16. The method of claim 15, wherein the data contained in the certificate
2 includes a subject identity and a serial number, and wherein the unique certificate reference is
3 computed from the subject identity and the serial number.

1 17. In a public key authentication system comprising a sender, a recipient,
2 a public key infrastructure and a network, a method of authenticating a message sent by the
3 sender to the recipient, the method comprising:

4 at the sender side:

5 digitally signing a message using a first private key belonging to the
6 sender;

7 retrieving a first certificate reference associated with a first certificate,
8 the first certificate including a first public key corresponding to the first private key, wherein
9 the first certificate and the associated first certificate reference are stored in the public key
10 infrastructure; and

11 transmitting a message comprising the digitally signed message and
12 the first certificate reference to the recipient via the network; and

13 at the recipient side:

14 receiving the message;

15 transmitting the first certificate reference to the public key

16 infrastructure via the network;

17 receiving the first certificate from the public key infrastructure via the
18 network; and

19 authenticating the digitally signed message using the first public key.

1 18. A public key infrastructure comprising:

2 a data store containing at least one certificate, wherein each of the at least one
3 certificate is associated with a different one of at least one certificate reference; and

4 a server coupled to the data store,

5 wherein the server is configured to receive a certificate, to compute a
6 certificate reference for the received certificate from data included in the certificate, and to
7 store the received certificate in association with the computed certificate reference in the data
8 store, and

9 wherein the server is further configured to respond to a request for a
10 certificate, the request including a received certificate reference, by identifying and providing
11 the one of the at least one stored certificate associated with the received certificate reference.

1 19. An electronic communication system comprising:

2 a public key infrastructure configured to store a plurality of certificates, to
3 associate with each of the plurality of certificates a different one of a plurality of certificate
4 references, and in response to a request including one of the plurality of certificate references,
5 to return the corresponding one of the plurality of certificates;
6 a sender configured to digitally sign a message using a first private key and to
7 send a message including the digitally signed message and a first certificate reference; and
8 a recipient configured to receive the message, to send a request including the
9 first certificate reference to the public key infrastructure, to receive a corresponding first
10 certificate from the public key infrastructure, and to use the first certificate to authenticate the
11 digitally signed message.